

T_Open

Securely specify and protect target filename.

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3356 bytes

Attack Category	<ul style="list-style-type: none">• Path spoofing or confusion problem		
Vulnerability Category	<ul style="list-style-type: none">• Indeterminate File/Path		
Software Context	<ul style="list-style-type: none">• Networking		
Location	<ul style="list-style-type: none">• xti.h		
Description	<p>The <code>t_open()</code> function must be called as the first step in the initialization of a transport endpoint. This function establishes a transport endpoint by supplying a transport provider identifier that indicates a particular transport provider (that is, transport protocol) and returning a file descriptor that identifies that endpoint. The argument name points to a file name that identifies a transport provider.</p> <p>If the communication is potentially sensitive, then it is important that no untrustworthy party can specify the file name or substitute an unauthorized file or device corresponding to the specified name.</p>		
APIs	Function Name		Comments
	t_open		
Method of Attack	<p>If an attacker can specify an unauthorized file or device, the program could be made to communicate insecurely. The attacker could tamper with or monitor the communication.</p>		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Whenever <code>t_open</code> is used.	For the communication to be secure, the filename passed to <code>t_open()</code> must be specified in a secure fashion, and the	Effective with respect to the identified issue, though other communication vulnerabilities may still exist.

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

		referenced file or device must be secured from tampering.	
Signature Details	int t_open(const char *name, int oflag, struct t_info *info);		
Examples of Incorrect Code	int fd = t_open(insecurelySpecifiedName, flag, info);		
Examples of Corrected Code	int fd = t_open("/dev/ securedNameForSecuriedDevice", flag, info);		
Source References	<ul style="list-style-type: none">• ITS4 Source Code Vulnerability Scanning Tool²• http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/ucd-ecs-95-09.pdf³		
Recommended Resource	<ul style="list-style-type: none">• man page for t_open()⁴		
Discriminant Set	Operating System	<ul style="list-style-type: none">• UNIX	
	Languages	<ul style="list-style-type: none">• C• C++	

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>